АНАЛИТИЧЕСКИЙ ОТЧЕТ

«Об образовании специалистов по информационной безопасности в Российской Федерации»

подготовлен экспертной подгруппой
по кибербезопасности НТИ «Энерджинет»

2021

Оглавление

Аннотация

Настоящий отчет подготовлен экспертами группы Кибербезопасность направления «Энерджинет» Национальной технологической инициативы с целью выявления наиболее острых проблем в области обеспечения подготовки специалистов по информационной безопасности в Российской Федерации, формирования комплексного взгляда на состояние образования, учитывающего мнения работодателей, профессионального сообщества и обучающихся.

В настоящее время в отношении образования в области информационной безопасности складываются противоречивые мнения, высказываемые как официально, в рамках различных форумов, так и неофициально, в том числе в частном порядке. В частности, как полярное высказывается мнение о неспособности региональных вузов (или, в более общей форме, всех вузов) подготовить специалистов, способных хотя бы на минимальном уровне обеспечить потребности государственных, муниципальных органов власти, специализированных компаний.

В отчете приведены результаты анализа анонимного опроса, проводимого среди участников сообществ специалистов по информационной безопасности в Telegram и Facebook. Общее число респондентов 269 чел. Представляется, что именно анонимность опроса, независимого от конъюнктуры среды или работы в конкретном предприятии или вузе, обеспечивает объективность его результатов.

Необходимо отметить, согласно тематикам сообществ, допускаем, что респонденты, принявшие участие в опросе, в целом являются специалистами в области информационной безопасности, в основном представляют компании, работающие в области информационной безопасности, и являются потенциальными или фактическими работодателями для студентов, обучающихся по специальностям в области информационной безопасности. Полные данные, описывающие респондентов, приведены в Приложении 1.

ЦЕЛЬЮ ОПРОСА ЯВЛЯЕТСЯ:

1. Четкое определение актуальных проблем подготовки специалистов в области информационной безопасности.

2. Выработка конструктивных подходов к решению выявленных проблем.

Отчет предназначен для руководителей и специалистов, работающих в сфере информационной безопасности.

Структура образования специалистов по информационной безопасности в Российской Федерации

Структура системы образования, описанная в ст.10 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», состоит из системы образования, вида и уровня образования. Основой объективной оценки соответствия установленным требованиям образовательной деятельности и подготовки обучающихся, освоивших образовательные программы соответствующего уровня и соответствующей направленности, независимо от формы получения образования и формы обучения, являются федеральные государственные образовательные стандарты.

Внешняя оценка качества образовательной деятельности и подготовки обучающихся по основной образовательной программе может осуществляться в рамках профессионально-общественной аккредитации, проводимой работодателями, их объединениями, а также уполномоченными ими организациями, в том числе иностранными организациями, либо авторизованными национальными профессионально-общественными организациями, входящими в международные структуры, с целью признания качества и уровня подготовки выпускников, отвечающими требованиям профессиональных стандартов (при наличии), требованиям рынка труда к специалистам соответствующего профиля.

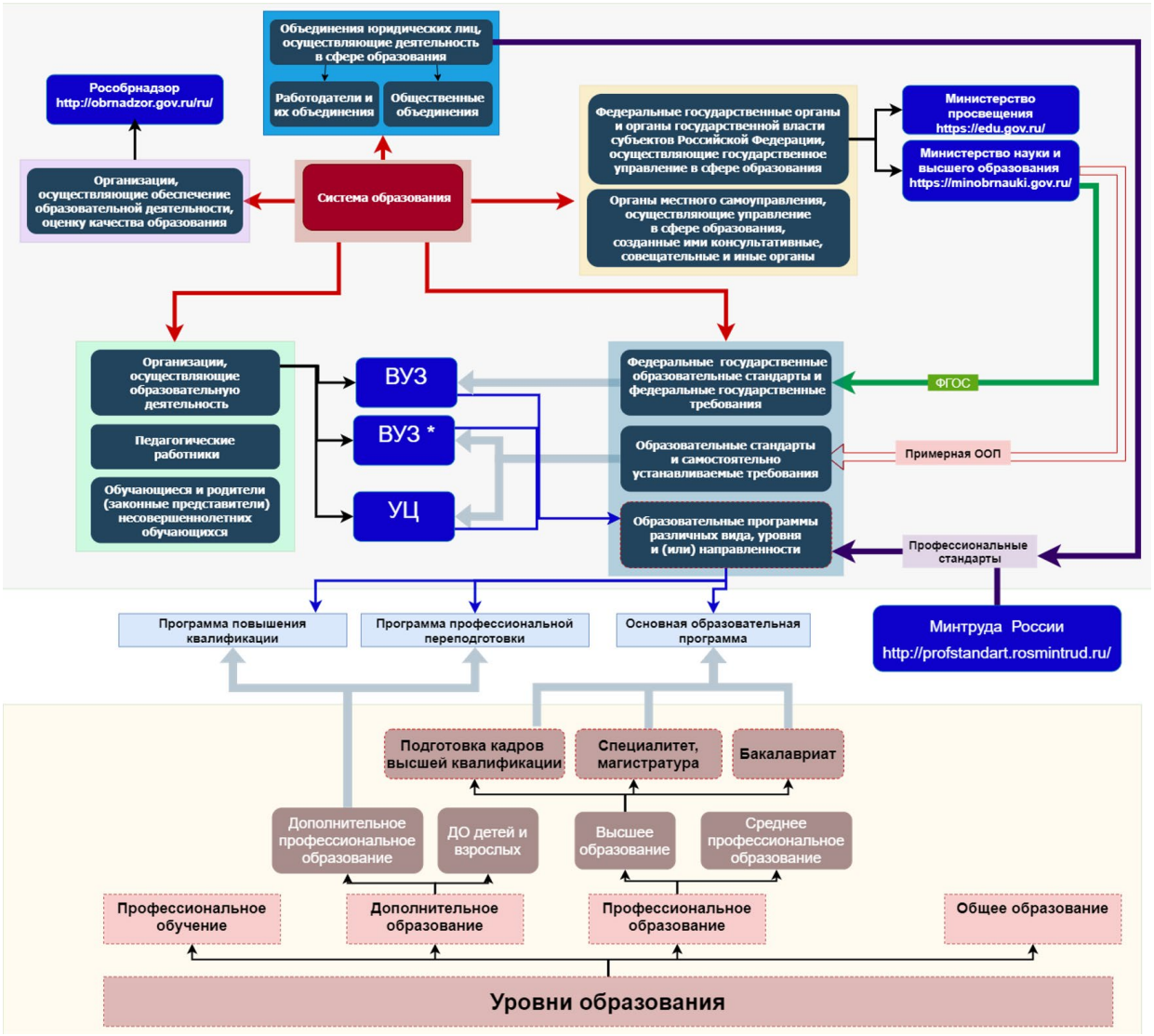


Схема 1. Структура системы образования

*ВУЗ - Московский государственный университет имени М.В. Ломоносова, Санкт-Петербургский государственный университет, образовательные организации высшего образования, в отношении которых установлена категория «федеральный университет» или «национальный исследовательский университет», а также федеральные государственные образовательные организации высшего образования, перечень которых утверждается указом Президента Российской Федерации, вправе разрабатывать и утверждать самостоятельно образовательные стандарты по программам бакалавриата, программам специалитета, программам магистратуры, программам ординатуры и программам ассистентуры-стажировки. Требования к условиям реализации и результатам освоения образовательных программ высшего образования, включенные в такие образовательные стандарты, не могут быть ниже соответствующих требований федеральных государственных образовательных стандартов.

В целом образовательный процесс в организации осуществляется на основании образовательных программ различного вида, уровня и (или) направленности. Образовательная программа представляет собой систему документов, разработанную с учетом потребностей регионального рынка труда, на основе федерального государственного образовательного стандарта высшего образования по определенному направлению подготовки, и содержит основные характеристики образования (объем, содержание, планируемые результаты), организационно-педагогические условия, формы аттестации, которые представлены в виде: учебного плана, календарного учебного графика, рабочих программ дисциплин, программ практик, программы итоговой (государственной итоговой) аттестации, а также оценочных и методических материалов.

Выпускники образовательной программы готовятся к осуществлению профессиональной деятельности в соответствии с требованиями профессионального стандарта.

При определении профессиональных компетенций на основе профессиональных стандартов Организация осуществляет выбор профессиональных стандартов, соответствующих профессиональной деятельности выпускников, из числа указанных в приложении к ФГОС ВО и (или) иных профессиональных стандартов, соответствующих профессиональной деятельности выпускников, из реестра профессиональных стандартов (перечня видов профессиональной деятельности), размещенного на специализированном сайте Министерства труда и социальной защиты Российской Федерации «Профессиональные стандарты» (http://profstandart.rosmintrud.ru) (при наличии соответствующих профессиональных стандартов). Из каждого выбранного профессионального стандарта Организация выделяет одну или несколько обобщенных трудовых функций (далее - ОТФ), соответствующих профессиональной деятельности выпускников, на основе установленных профессиональным стандартом для ОТФ уровня квалификации и требований раздела «Требования к образованию и обучению». ОТФ может быть выделена полностью или частично.

По состоянию на август 2021 года в Российской Федерации действуют 5 открытых профессиональных стандартов в области информационной безопасности и два стандарта, содержащих сведения ограниченного доступа.

В настоящее время ведется разработка и публичное обсуждение 8 проектов новых и обновленных старых профессиональных стандартов. Перечень стандартов и проектов представлен в Таблице 1.

№	Код	Наименование	Год утверждения
1	**Профессиональные стандарты**		
1.1	06.030	Специалист по защите информации в телекоммуникационных системах и сетях	2016
1.2	06.031	Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности	2016
1.3	06.032	Специалист по безопасности компьютерных систем и сетей	2016
1.4	06.033	Специалист по защите информации в автоматизированных системах	2016
1.5	06.034	Специалист по технической защите информации	2016
2	**Проекты профессиональных стандартов**		
2.1		Специалист по информационной безопасности в кредитно-финансовой сфере	
2.2		Специалист по обеспечению безопасности значимых объектов критической информационной структуры	
2.3		Специалист по технической защите информации	
2.4		Специалист по защите информации в телекоммуникационных системах и сетях	
2.5		Специалист по защите информации в автоматизированных системах	
2.6		Специалист по безопасности компьютерных систем и сетей	
2.7		Специалист по криптографической деятельности	
2.8		Специалист по автоматизации информационно-аналитической деятельности	
3	**Профессиональные стандарты, содержащий сведения, составляющие государственную тайну, или сведения конфиденциального характера**		
3.1	12.004	Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак	2016
3.2	12.005	Специалист по противодействию иностранным техническим разведкам	2016

Таб. 1. Перечень профессиональных стандартов в области информационной безопасности

[1] С текстом стандартов и проектов можно ознакомиться на ресурсе Минтруда, https://profstandart.rosmintrud.ru, сайте Центрального банка Российской Федерации, https://cbr.ru/ и на сайте Межрегиональной общественной организации «Ассоциация защиты информации», https://azi.ru.

В общем случае профессиональные стандарты в области информационной безопасности носят рекомендательный характер. Исключения предусмотрены в следующих случаях.

Согласно части второй статьи 57 ТК РФ наименование должностей, профессий, специальностей и квалификационные требования к ним должны соответствовать наименованиям и требованиям, указанным в квалификационных справочниках или профессиональных стандартах, если в соответствии с ТК РФ или иными федеральными законами с выполнением работ по этим должностям, профессиям, специальностям связано предоставление компенсаций и льгот либо наличие ограничений.

Согласно статье 195.3 ТК РФ требования к квалификации работников, содержащиеся в профессиональных стандартах, обязательны для работодателя в случаях, если они установлены ТК РФ, другими федеральными законами, иными нормативными правовыми актами Российской Федерации.

На основании действующих профессиональных стандартов разработаны 13 федеральных государственных образовательных стандартов (ФГОС), охватывающих все уровни образования начиная со среднего специального и заканчивая высшей квалификацией. Перечень ФГОС представлен в Таблице 2.

№	Код	Наименование	Год утверждения
1	**Среднее профессиональное образование**		
1.1	10.02.01	Организация и технология защиты информации	2014
1.2	10.02.02	Информационная безопасность телекоммуникационных систем	2014
1.3	10.02.03	Информационная безопасность автоматизированных систем	2014
1.4	10.02.04	Обеспечение информационной безопасности телекоммуникационных систем	2016
1.5	10.02.05	Обеспечение информационной безопасности автоматизированных систем	2016
2	**Бакалавриат**		
2.1	10.03.01	Информационная безопасность	2016
3	**Магистратура**		
3.1	10.04.01	Информационная безопасность	2016
4	**Специалитет**		
4.1	10.05.01	Компьютерная безопасность	2016
4.2	10.05.02	Информационная безопасность телекоммуникационных систем	2016
4.3	10.05.03	Информационная безопасность автоматизированных систем	2016
4.4	10.05.04	Информационно-аналитические системы безопасности	2016
4.5	10.05.05	Безопасность информационных технологий в правоохранительной сфере	2016
5	**Аспирантура**		
5.1	10.06.01	Информационная безопасность	2014

Таб. 2. Перечень ФГОС в области информационной безопасности

В Приложении 2 представлен перечень должностей и их трудовых функций, предусмотренных действующими профессиональными стандартами, а также требования к уровню образования специалистов.

[2] С текстом ФГОС можно ознакомиться на ресурсе Национальной ассоциации развития образования и науки, https://fgos.ru/

Результаты исследования

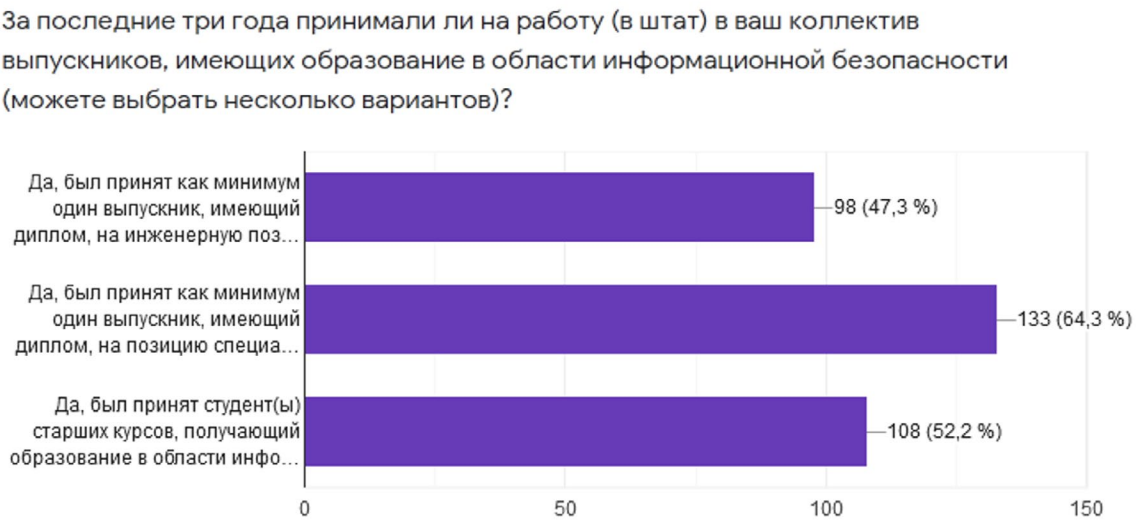
Основной посыл, с которого предлагается начать изложение анализа результатов опроса – это общая неудовлетворенность качеством образования. При ответах на вопросы подавляющее большинство опрошенных отметило недостаточность практических и(или) теоретических знаний выпускников.

То, что такое мнение сложилось в условиях непосредственного общения с выпускниками, можно видеть из следующих данных: 207 респондентов за последние 3 года принимали на работу выпускников, имеющих образование в области информационной безопасности (можно было выбирать несколько вариантов ответов). Согласно опросу:

47,3%
были приняты на инженерную позицию;

64,3%
были приняты на позицию специалиста;

52,2%
были приняты на стажерскую позицию.



Значительную долю — 45% опрошенных составили потребители ИБ и ИТ услуг. Данные лица фактически выступают в двух ипостасях: как конечные заказчики результатов внедрения ИБ-решений и как работодатели для специалистов, которые должны принимать и сопровождать данные решения. При этом интересно отметить то, что 74% опрошенных заинтересованы в создании систем защиты/безопасности информационных систем своими силами, соответственно, в наличии собственных специалистов в области проектирования и внедрения, не только контроля и эксплуатации.

Таким образом разница в доле респондентов, выступающих в качестве потребителей услуг, и доле респондентов, заинтересованных в создании систем защиты собственными силами, говорит о явно выраженной тенденции отказа от аутсорсинга услуг по информационной безопасности на уровне заинтересованных специалистов. Это может косвенно свидетельствовать об определенном недоверии к уровню предлагаемых продуктов в сфере ИБ (услуг, проектов, сдаваемых в эксплуатацию систем), обусловленных, в том числе, качеством подготовки специалистов.

Даже при условии заказа систем защиты у подрядчиков, с точки зрения образования остается актуальным вопрос обучения процедурам контроля создания ими таких систем, а с точки зрения заказчика – наличия таких специалистов, методик и систем контроля. Такой интерес вполне объясним, так как даже при привлечении подрядчиков для решения задач создания систем защиты/безопасности, ответственность перед законом всё равно в полном объеме несет заказчик, подрядчик же отвечает перед заказчиком лишь в рамках договорных отношений.

Следующим моментом, на который следовало бы обратить внимание, является то, что в образовательных стандартах ключевым является сочетание общепрофессиональных и профессиональных компетенций. Для практической работы важно сочетание профессиональных компетенций и знаний предметной области. Поэтому понимание и требования к специалистам по информационной безопасности трансформируется от общего к частным. Требуются специалисты, которые имеют компетенции и знания, учитывающие отраслевую специфику. Как следствие, 75% опрошенных утверждают, что образование должно содержать больше отраслевой специфики.

Согласно опросу выпускники соответствуют требованиям работодателя (полностью или в большей части) только примерно в 15% случаев. Значит, они должны либо самостоятельно, либо под руководством специалистов организации суметь адаптироваться под требования организации, куда их после выпуска приняли на работу. Соответственно, здесь уже играет роль не только набор конкретных знаний и умений, а способность адаптироваться к изменяющимся обстоятельствам.

Вовлеченность специалистов в систему образования

88,1 % опрошенных знают про существование образовательных стандартов (диаграмма 1).

При это лишь **43,9 %** опрошенных читали образовательные стандарты

10,9% считают, что от образовательных стандартов что-то зависит (диаграмма 2).

Диаграмма 1.
Знание образовательных стандартов

Диаграмма 2.
Роль образовательных стандартов

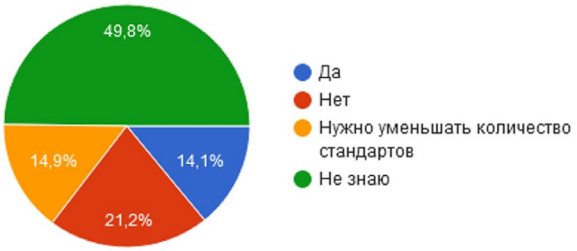


Диаграмма 3.
Необходимость в изменении образовательных стандартах

Диаграмма 4.
Готовность участвовать в разработке образовательных стандартов

Система подготовки специалистов

Если проанализировать требования к уровню образования для различных должностей (Приложение 2), а также требования нормативных правовых актов (НПА) к специалистам по информационной безопасности, работающим в сферах безопасности критической информационной инфраструктуры, технической защиты конфиденциальной информации и средств криптографической защиты информации, появляется определенный диссонанс.

Так НПА требуют от специалистов (включая руководителей профильных подразделений) иметь высшее профессиональное образование по направлению подготовки «Информационная безопасность» в соответствии с Общероссийским классификатором специальностей и стаж работы, или высшее образование, стаж работы и профессиональную переподготовку. Наличие степени Бакалавра удовлетворяет этим требованиям. Вместе с тем, все профессиональные стандарты для Бакалавров предусматривают только начальные должности.

Также в ходе бесед и выступлений рядом специалистов высказываются сомнения в необходимости подготовки бакалавров по направлению ИБ, предлагается или ИБ-специалитет, или бакалавриат по технической специальности (например, ИТ для компьютерной безопасности или радиотехника для ТЗИ) плюс магистратура по ИБ.

Что касается специализации, то мнение опрошенных разделились почти поровну в отношении необходимости подготовки более узкоспециализированных специалистов.

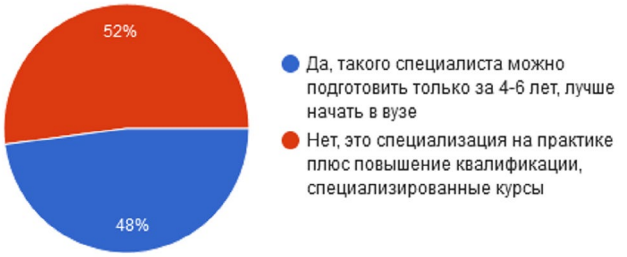


Диаграмма 5.
Необходимость узкой специализации образовательных

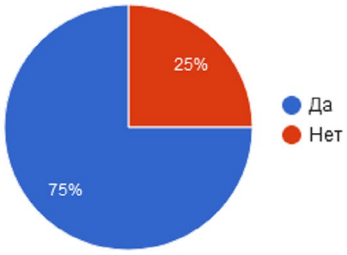


Диаграмма 6.
Необходимость отраслевой специфики в образование

Диаграмма 7.
Необходимость бакалавров

Диаграмма 8.
Соответствие подготовки выпускников требованиям работодателей

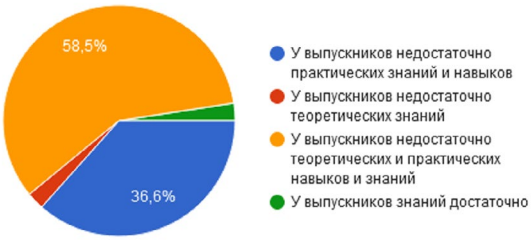


Диаграмма 9.
Оценка подготовленности выпускников

Послевузовское образование

В соответствии с нормативными правовыми актами Российской Федерации работодатели обязаны проводить обучение и повышение квалификации работников по направлению информационной безопасности. В частности, в соответствии с п.15 требований, утвержденных приказом ФСТЭК России от 21 декабря 2017 г. № 235 *Субъект критической информационной инфраструктуры должен проводить* ***не реже одного раза в год*** *организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности критической информационной инфраструктуры и о возможных угрозах безопасности информации.*

В соответствии с п. 18.6 требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17 *Периодичность проведения практических занятий и тренировок с персоналом, мероприятий по обучению персонала и контролю осведомленности персонала устанавливается оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационной системы, но* ***не реже 1 раза в два года***.

В соответствии с пп. б) п. 6) положениями о лицензировании, утвержденными ПП РФ от 03.02.2012 № 79 и ПП РФ от 03.03.2012 № 171 повышение квалификации по лицензируемому *виду деятельности лиц, указанных в подпункте «а» настоящего пункта,* ***не реже одного раза в 5 лет.***

82,4% работодателей респондентов обеспечивают обучение работников. Только у 30,5% опрошенных отсутствует внутреннее обучение по ИБ.

Диаграмма 10.
Оплата обучения работодателем

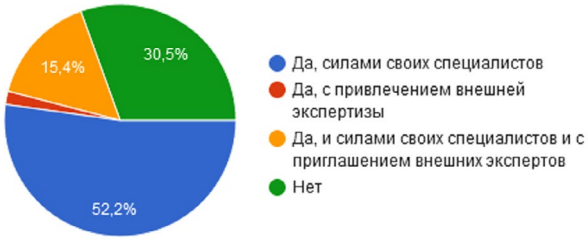


Диаграмма 11.
Внутреннее обучение по ИБ

72,6% специалистов готовы самостоятельно оплачивать повышение своей квалификации. При этом, почти 50% опрошенных предпочитают повышать квалификацию на соответствующих курсах, 38% - самостоятельно

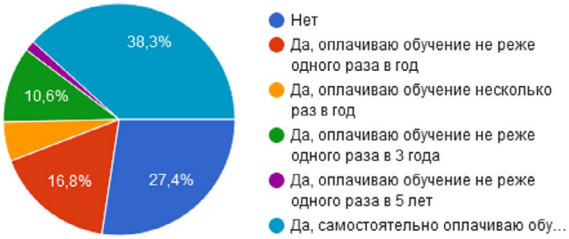


Диаграмма 12.
Самостоятельная оплата обучения

Диаграмма 13.
Приоритетный способ повышения квалификации

Половина респондентов более заинтересована в обучении способам и средствам реализации отдельных технических мер защиты, при этом обеспечение соответствия требованиям законодательства, нормативных правовых актов, нормативно-технической документации Российской Федерации заинтересовало вдвое меньше опрошенных. Обучение же обеспечению соответствия положениям международных стандартов и лучших практик оказалось наиболее интересно 14 процентам опрошенных.

Диаграмма 14.
Приоритетные направления обучения

Диаграмма 15.
Приоритетные типы курсов повышения квалификации

Примечательно, что как показали ответы на предыдущий вопрос, обеспечение соответствия требованиям законодательства, нормативных правовых актов, нормативно-технической документации Российской Федерации интересно также четверти респондентов.

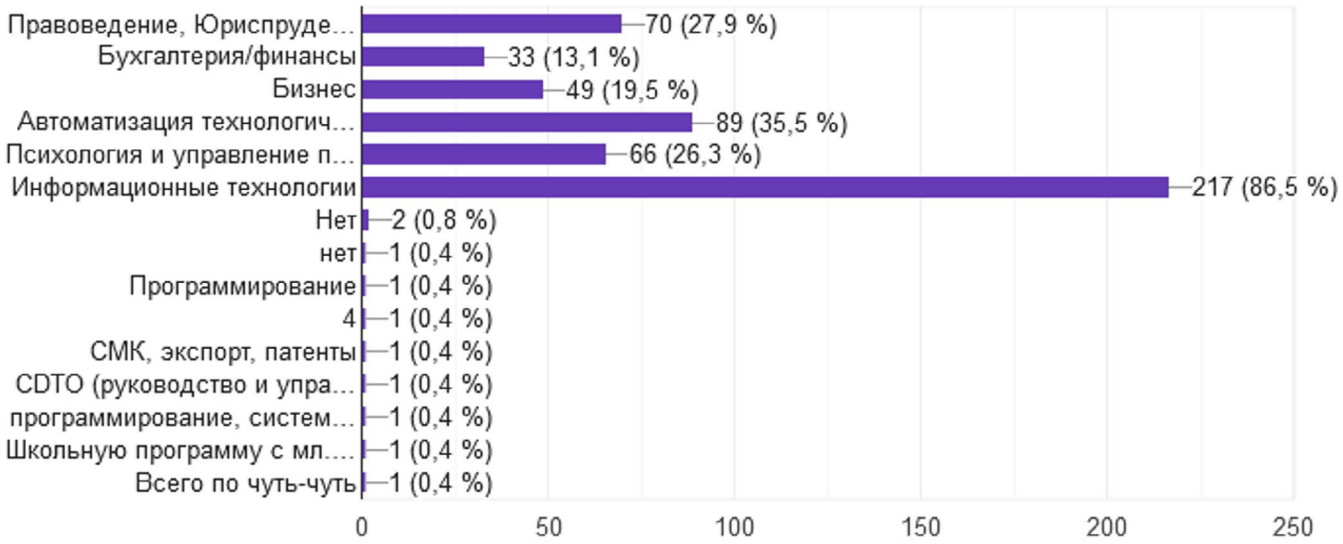
Как оказалось, более трёх четвертей респондентов в той или иной мере заинтересованы обучаться на базе иностранных материалов и практик, и лишь 22 процента сконцентрированы лишь на российских источниках.

Диаграмма 16.
Комфортность изучения зарубежных документов

Диаграмма 17.
Разнообразие курсов на русском языке

Диаграмма 18.
Качество курсов на русском языке

Изучение смежных отраслей специалистами:



Тренды в изучении смежных специальностей хорошо отражают потребности рынка в новых типах специалистов, сочетающих в себе знания и умения из различных областей, а также потребности в эффективной коммуникации с бизнесом.

Так, с бурным развитием интернет-сервисов выросли требования к обеспечению безопасности разрабатываемого программного обеспечения, что в свою очередь привело к выделению нового класса специалистов по безопасной разработке, сочетающих в себе квалификации специалиста по безопасности и разработчика программного обеспечения;

Вопросы защиты персональных данных, обрабатываемых глобальными интернет-сервисами, привели к появлению специалистов по приватности, безопасности и защите данных (DPO — Data Protection Officer), владеющих навыками специалиста по безопасности и юриста.

Популяризация технологий Интернета вещей и цифровая трансформацияинженерныхитехнологическихсистемпривела к спросу на специалистов по безопасности автоматизированных систем управления технологическими процессами, сочетающих в себе квалификации специалистов по безопасности и инженеров автоматизации.

Смещение концепций информационной безопасности в сторону защиты человека, как самого слабого звена, ведут к необходимости появления специалистов по повышению осведомленности, сочетающих в себе специалистов по безопасности, психологов и преподавателей.

Анализ результатов исследования

Подготовка специалистов осуществляется на основании образовательных стандартов, соответствующих действующим профессиональным стандартам.

Разработчиками действующих профессиональных стандартов являются:

- ФГУП «Научно-технический центр «Атлас» (ФГУП «НТЦ «Атлас»);
- ФГКОУ ВО «Академия Федеральной службы безопасности Российской Федерации»;
- ФГАОУ ВО «Национальный исследовательский университет «Московский институт электронной техники»;
- Федеральное учебно-методическое объединение по укрупненной группе специальностей и направлений подготовки «Информационная безопасность»;
- ЗАО «Ассоциация специалистов информационных систем»;
- Межрегиональная общественная организация «Ассоциация защиты информации».

Таким образом, действующие профессиональные стандарты разработаны представителями специальных служб, образовательных учреждений и общественных организаций, объединяющих производителей средств защиты информации и интеграторов услуг.

Представители государственных и коммерческих организаций по сути являющиеся основными потребителями трудовых ресурсов не участвовали в формировании «заказа» - перечня профессиональных и специальных требований - на подготовку специалистов по информационной безопасности.

Если проанализировать обобщенные трудовые функции профессиональных стандартов (Приложение 2) становится виден явный перекос в сторону специалистов, работающих в специальных службах, производителях средств защиты информации и в компаниях, оказывающих услуги информационной безопасности, что также косвенно подтверждает слабое участие потребителей ИБ продуктов и услуг в формировании требований к специалистам по ИБ.

Также стоит отметить проблему с отсутствием у преподавательского состава практического опыта обеспечения информационной безопасности.

Учитывая существенную разницу в уровне заработной платы преподавателей ВУЗов и специалистов по информационной безопасности, стоит констатировать факт невозможности обеспечить ВУЗ профессиональными преподавателями, способными давать студентам актуальные знания и умения в условиях стремительного развития сферы информационной безопасности.

Нивелировать данную проблему может позволить более активное участие практикующих специалистов по информационной безопасности в образовательной деятельности ВУЗов. При этом образовательная деятельность - это дорога с двусторонним движением, позволяющая преподающему наращивать свои компетенции в не меньшей степени чем студенту.

Оснащенность ВУЗов современными стендами с программными и программно-аппаратными средствами.

По состоянию на сентябрь 2021 года в открытых реестрах сертифицированных средств защиты информации совокупно содержатся 2421 программных, программно-аппаратных и аппаратных средств защиты информации.

Из них сертифицировано ФСБ России:

- 23 операционные системы;
- 8 образцов мультипротокольного оборудования;
- 1 средство аудита информационной безопасности;
- 9 средств обнаружения компьютерных атак;
- 18 межсетевых экранов;
- 15 антивирусных средств;
- 245 средств криптографической защиты информации, из которых 86 - программные и программно-аппаратные средства VPN.

Из них сертифицировано ФСТЭК России:

- 18 средств доверенной загрузки;
- 125 межсетевых экранов;
- 46 средств обнаружения вторжения;
- 20 операционных систем;
- 34 средства антивирусной защиты.

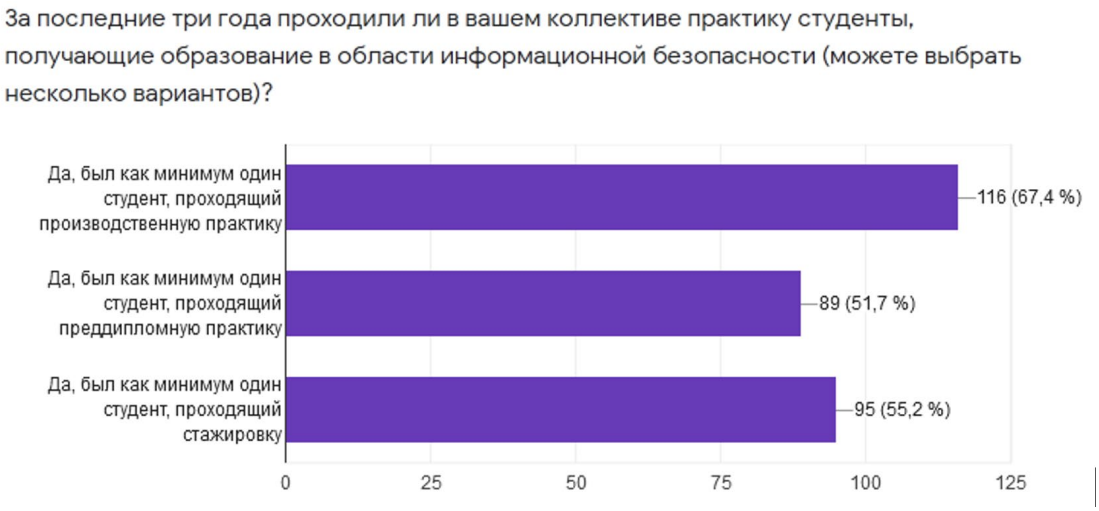
Далеко не каждый вуз может позволить себе обеспечить наличие материальной, технической и методической базы и трудовых ресурсов для предоставления студентам возможности ознакомления с указанными сертифицированными средствами защиты информации. А на практике в организациях применяются более широкий перечень средств, включая и несертифицированные средства защиты.

Без предоставления студентам возможности ознакомления с современными средствами обеспечения безопасности невозможно обеспечить достаточный уровень практических знаний у выпускников.

Решение данной проблемы находится за пределами вузов. Необходимо создание и предоставление студентам бесплатного доступа к национальным полигонам, позволяющим студентам отрабатывать практические задачи по эксплуатации всех имеющихся на рынке средств защиты.

Немаловажным фактором в образовании помимо качества программ обучения, преподавательского состава и технической оснащенности ВУЗов является наличие возможности прохождения студентами производственной и преддипломной практики на реальных предприятиях, а не выполнение синтетических задач на профильных кафедрах.

А насколько профессиональное сообщество и предприятия готовы принимать практикантов?



Выводы

Успешное развитие образования специалистов по информационной безопасности в Российской Федерации требует осознанного участия всех заинтересованных сторон, включая представителей государственных и частных организаций, в интересах которых в конечном итоге и будут трудиться специалисты.

На основании анализа предметной области отмечено изменение свойств защищаемых объектов, а значит и подходов к обеспечению их информационной безопасности, не нашедших на момент их применения отражения в нормативной базе. Следствием из сформулированных рассуждений является необходимость иметь в учебном плане предметы, позволяющие сформировать у студентов понимание фундаментальных основ информационной безопасности, ее базовых механизмов. Как представляется, указанные знания должны применяться выпускниками в случае необходимости перестройки функциональных процессов и без получения от регуляторов или заказчиков конкретных указаний по решению возникших производственных задач.

Это приводит к определенному противоречию — система подготовки кадров ориентируется в основном на внутренние документы, а предприятия предпочитают рассматривать ещё и зарубежные типовые практики и решения.

Более того, в научной литературе и учебных пособиях отсутствует сравнительный критический анализ российских и зарубежных подходов к обеспечению ИБ и разработке методик специалистов, что впоследствии порождает дискуссии между специалистами, прошедшими различные школы.

Представляется целесообразным силами академического сообщества при поддержке экспертов и компаний, работающих в сфере ИБ, подготовить учебное пособие или программу дополнительного профессионального образования, в котором будет отражена приоритезация целей, задач информационной безопасности со стороны российских и зарубежных специалистов, дан обзор подходов к ее обеспечению и приведена методология их совокупного анализа для принятия решений.

С точки зрения регуляторов одним из ключевых моментов в обеспечении качества образования являются профессиональные и образовательные стандарты, точнее их связка. Опрос показал, что в целом респонденты знают о существовании образовательных стандартов, но не считают их важным фактором обеспечения качества образования, всего 10% опрошенных согласились с важностью стандартов. При этом готовность участвовать в доработке образовательных стандартов отметили только 40% опрошенных. Учитывая рекомендательный характер профессиональных стандартов, на которые ориентируются при создании ФГОС, представляется целесообразными крупнейшим работодателям и вендорам сместить акцент своего внимания на учебные планы конкретных вузов, чьих выпускников они планируют или предпочитают нанимать на работу.

В качестве итога данного краткого обзора можно отметить следующее. Основная неудовлетворенность качеством образования формируется со стороны работодателей. Вместе с тем, только незначительная доля компаний, работающих в сфере ИБ, участвует в формировании обратной связи и непосредственно в базовой – вузовской – подготовке специалистов. Представляется, что более активное участие компаний в образовательной деятельности в сфере ИБ (в различных формах) позволит в целом вывести качество образования на новый уровень.

Отчет подготовлен рабочей группой в составе:
А.А. Боровский, А.В. Петухов, Д.И. Правиков, С.Ю. Петрова, М.Б. Смирнов, А.Ю. Юршев., Д. Р. Ли

Приложение 1

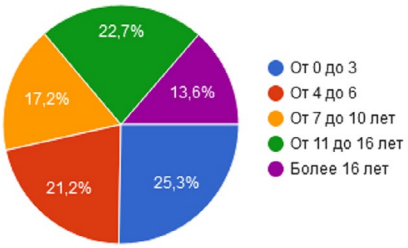
Целевая аудитория опроса и общие характеристики респондентов

Благодарим администрацию и участников сообществ
за активное участие в опросе!

Наименование	Ссылка
КИИ 187-ФЗ	https://t.me/KII187FZ
152-ФЗ и Персональные данные	https://t.me/fz152pdn
Все ФЗ (vseFZ)	https://t.me/vseFZ
ПДн 152-ФЗ	https://t.me/PDn152FZ
Cyberconf	https://t.me/cyberconf
RUSCADASEC community: Кибербезопасность АСУ ТП	https://t.me/RuScadaSec
ИБ в Финсекторе	https://t.me/FinSecurity
Дом советов	https://t.me/dom_sovetov_rupor
Прайваси Чат	https://t.me/privacy_chat
SOC Технологии	https://t.me/phd_soc
Цифровая подстанция	https://t.me/releyshik
Межрегиональная общественная организация Ассоциация руководителей служб информационной безопасности, АРСИБ	http://aciso.ru/

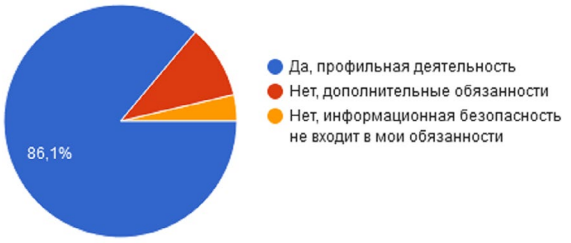
Кем является Ваша организация?

Каков Ваш стаж в информационной безопасности?



Какова Ваша роль в организации?

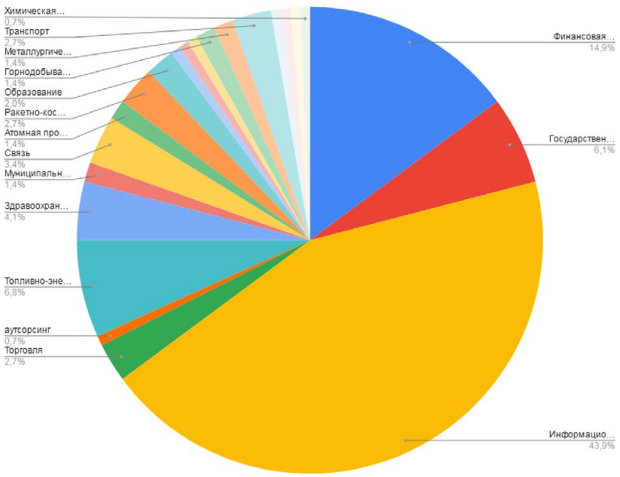
Информационная безопасность для Вас профильная деятельность?



У вас профильное образование по информационной безопасности (специалист, магистр, бакалавр, техник)?

К какому поколению Вы относитесь?

К какой отрасли относится Ваша организация?



Приложение 2

Должности и трудовые функции, предусмотренные профессиональными стандартами в сфере информационной безопасности

№	Требования к образованию и обучению	Возможные наименования должностей, профессий	Обобщенные трудовые функции
1	**Специалист по защите информации в телекоммуникационных системах и сетях**		
1.1	Среднее профессиональное образование	Техник по защите информации I категории Техник по защите информации II категории Техник по защите информации Старший техник по обслуживанию телекоммуникационного оборудования	Выполнение комплекса мер по обеспечению функционирования СССЭ и (за исключением сетей связи специального назначения) и средств их защиты от НСД
1.2	Бакалавриат	Инженер по защите информации Инженер по телекоммуникациям Администратор телекоммуникационного оборудования	Обеспечение защиты от НСД сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации
1.3	Бакалавриат и повышение квалификации	Инженер специальной связи Инженер по защите информации	Обеспечение функционирования средств связи сетей связи специального назначения
1.4	Специалитет или магистратура	Инженер-программист I категории Инженер-программист II категории Инженер-программист III категории Инженер-программист Инженер-проектировщик I категории Инженер-проектировщик II категории Инженер-проектировщик III категории Инженер-проектировщик Руководитель проектов Специалист по защите информации I категории Специалист по защите информации II категории Специалист по защите информации	Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД
1.5	Специалитет или магистратура	Старший инженер Старший инженер-разработчик Старший инженер специальной связи Консультант по специальным телекоммуникациям	Обеспечение защиты средств связи сетей связи специального назначения от НСД
1.6	Специалитет или магистратура	Начальник (руководитель) отдела (отделения) систем защиты информации Ведущий инженер-разработчик	Управление развитием средств и систем защиты СССЭ от НСД
1.6	Специалитет или магистратура	Начальник (руководитель) научно-исследовательского отдела (лаборатории) Ведущий (главный) специалист по защите информации Научный консультант по защите информации	Экспертиза проектных решений в сфере защиты СССЭ от НСД

2	Специалист по безопасности компьютерных систем и сетей		
2.1	Среднее профессиональное образование	Техник по безопасности компьютерных систем и сетей	Обслуживание средств защиты информации в компьютерных системах и сетях
2.2	Бакалавриат	Администратор безопасности компьютерных систем и сетей Администратор по обеспечению безопасности информации Инженер-программист по технической защите информации I категории Инженер-программист по технической защите информации II категории Инженер-программист по технической защите информации Инженер-программист I категории Инженер-программист II категории Инженер-программист III категории Инженер-программист	Администрирование средств защиты информации в компьютерных системах и сетях
2.3	Специалитет или магистратура	Специалист по защите информации в компьютерных системах и сетях Эксперт по анализу защищенности компьютерных систем и сетей Ведущий (старший) специалист по защите информации Руководитель группы (специализированной в прочих отраслях) Руководитель группы (функциональной в прочих областях деятельности)	Оценивание уровня безопасности компьютерных систем и сетей
2.4	Специалитет или магистратура и повышение квалификации или аспирантура	Главный специалист по защите информации Руководитель отдела систем защиты информации Заместитель руководителя департамента (отдела) исследований и разработок Руководитель департамента (отдела) исследований и разработок	Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей

3	Специалист по защите информации в автоматизированных системах		
3.1	Среднее профессиональное образование	Техник по защите информации I категории Техник по защите информации II категории Техник по защите информации	Обслуживание систем защиты информации в автоматизированных системах
3.2	Бакалавриат	Инженер по защите информации Специалист по защите информации I категории Специалист по защите информации II категории Специалист по защите информации Инженер-программист по технической защите информации I категории Инженер-программист по технической защите информации II категории Инженер-программист по технической защите информации Инженер-программист I категории Инженер-программист II категории Инженер-программист III категории Инженер-программист	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации
3.3	Бакалавриат	Инженер по защите информации Специалист по защите информации I категории Специалист по защите информации II категории Специалист по защите информации Инженер-программист по технической защите информации I категории Инженер-программист по технической защите информации II категории Инженер-программист по технической защите информации Инженер-программист I категории Инженер-программист II категории Инженер-программист III категории Инженер-программист	Внедрение систем защиты информации автоматизированных систем
3.4	Специалитет или магистратура	Ведущий инженер-разработчик систем защиты информации Ведущий специалист по защите информации Руководитель проектов в области разработки систем защиты информации Руководитель отдела систем защиты информации	Разработка систем защиты информации автоматизированных систем
3.5	Специалитет или магистратура и повышение квалификации или аспирантура	Главный специалист по защите информации Руководитель отдела систем защиты информации Заместитель руководителя департамента (отдела) исследований и разработок Руководитель департамента (отдела) исследований и разработок	Формирование требований к защите информации в автоматизированных системах

4	Специалист по технической защите информации		
4.1	Среднее профессиональное образование	Техник по технической защите информации I категории Техник по технической защите информации II категории Техник по технической защите информации	Проведение работ по установке и техническому обслуживанию средств защиты информации
4.2	Бакалавриат	Специалист по технической защите информации I категории Специалист по технической защите информации II категории Специалист по технической защите информации Инженер по технической защите информации	Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации Производство, сервисное обслуживание и ремонт средств защиты информации Проведение контроля защищенности информации
4.3	Специалитет или магистратура	Специалист по технической защите информации I категории Специалист по технической защите информации II категории Специалист по технической защите информации Инженер по технической защите информации	Разработка средств защиты информации Проектирование объектов в защищенном исполнении
4.4	Специалитет или магистратура и повышение квалификации	Специалист по технической защите информации I категории Специалист по технической защите информации II категории Специалист по технической защите информации Инженер по технической защите информации	Проведение аттестации объектов на соответствие требованиям по защите информации Проведение сертификационных испытаний средств защиты информации на соответствие требованиям по безопасности информации
4.5	Специалитет или магистратура и повышение квалификации или аспирантура	Главный специалист по технической защите информации Руководитель структурного подразделения по технической защите информации	Организация и проведение работ по технической защите информации